

Presentation submission for the 2005 Ottawa Workshop on: “New Challenges for Access Control”

Title: The Globus Authorization Processing Framework

Authors: Frank Siebenlist (Argonne National Laboratory), Takuya Mori (NEC Corp.), Rachana Ananthakrishnan (ANL), Liang Fang (Indiana Uni.), Tim Freeman (UofChicago), Kate Keahey (ANL), Sam Meder (ANL), Olle Mulmo (KTH), Thomas Sandholm (KTH)

Abstract: The Globus Alliance[1] coordinates the development of the Globus Toolkit (GT)[2], an open source web services toolkit with a set of infrastructure services specifically geared to facilitate the building of secure Grid applications[3][4][5]. As the GT is used by many different Grid applications and projects worldwide, it cannot mandate specific security technologies and mechanisms, and has to adopt a modular approach to accommodate the choices made by those responsible for deployment.

For example, identity and attribute assertions have to be supported in X.509 Identity and Attribute Certificate[6][7], Kerberos[8], and SAML Identity/Attribute Assertion formats[9], while the authorization policies can be expressed in for example XACML[10]/XrML[11] statements,

CAS[12][13]/XCAP[14]/SAML Authorization Decisions Assertions, VOMS[15]/PERMIS[16] ACs, SPKI[17] certificates, or X509 Proxy Certificates[18][19]. Furthermore, all these statements can either be available in local storage within the trusted computing base of the relying party, be pushed by other parties via SOAP headers [20] or Proxy Certificate embedding, be pulled from online services, or external attribute and authorization services can be queried through Shibboleth[21]/GGF-OGSA-Authz[22]/SAML or XACML-2 call-out interfaces. Lastly, depending on the mechanism deployed, the delegation of rights is expressed in different ways to accommodate a common requirement in Grid applications where subjects and services empower (other) services to act on their behalf.

In order to meet this complex set of requirements, we are in the progress of developing an authorization-processing framework that is able to handle and interpret all the different attribute and policy assertions, and authorization decisions in a generic and consistent manner. The architecture of the framework makes use of a Policy Decision Point (PDP) abstraction that conceptually resembles the one defined for XACML. A normalized request context and decision format is used such that this PDP can be modeled as a black box authorization decision oracle without explicit knowledge about the policy statements used for the evaluation, and without knowing the policy language in which those statements are expressed.

In the first step of the authorization processing, the received and collected assertions with their associated issuers are verified and validated. The resulting attribute statements with their issuer-subject information are subsequently translated and mapped by mechanism specific Policy Information Points (PIPs) into a common format that is presented to the PDPs. This format is compatible with the XACML request context attribute format.

In the second step, the external authorization services and the different authorization statements of the same mechanism and the same issuer are combined. For each such external service and set of statements, a mechanism-specific PDP instance is created, wrapping a native policy evaluator or a proxy/callout to the authorization service's EPR[23][24]. Note that the assertion issuer or the identity of the external service is explicitly associated with each PDP instance. The end result is a set of PDP instances where the different mechanisms are abstracted behind the common PDP interface.

The final step is the authorization evaluation, for which we have a Master-PDP that receives the request context that applies to the authorization request under consideration. This Master-PDP orchestrates the querying of each applicable PDP instance for authorization decisions. Pre-defined combination rules determine how the different results from the PDP instances are to be combined to yield a single decision. By using the issuer information associated with the different PDP instances, the Master-PDP is also able to query the individual PDP instances whether the issuer has delegated administrative rights to other subjects. This can be used to determine delegation decision chains, and establish authorization decisions based on rights delegation. Note that by using this approach, the Master-PDP can determine authorization decisions based on delegated rights without explicit support from the native policy language evaluators.

Our presentation will discuss our authorization framework, and provide details about the implementation, features and limitations. We would like to note that our framework is still a work in progress and that we very much welcome feedback and suggestions for improvement during the workshop.

References:

- [1] Globus Alliance, <http://www.globus.org>
- [2] Globus Toolkit, <http://www.globus.org/toolkit/>
- [3] Global Grid Forum (GGF), <http://www.ggf.org>
- [4] Open Grid Services Architecture, OGSA working group at Global Grid Forum (GGF), "<https://forge.gridforum.org/projects/ogsa-wg>"
- [5] Siebenlist, F., Nagaratnam, N., Welch, V., Neuman, C. "Security for Virtual Organizations". *In The GRID 2: Blueprint for a New Computing Infrastructure*, Morgan Kaufman, 2004.
- [6] Housley, R., Polk, W., Ford, W., and D. Solo, " Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile ", RFC 3280, April 2002.
- [7] Farrell, S. and Housley, R., "An Internet Attribute Certificate Profile for Authorization", RFC 3281, April 2002.
- [8] Kohl, J. and Neuman, C., " The Kerberos Network Authentication Service (V5)", RFC 1510, September 1993
- [9] OASIS Security Services (SAML) TC, "http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security"
- [10] OASIS eXtensible Access Control Markup Language (XACML) TC, "http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml"
- [11] eXtensible Rights Markup Language (XrML) 2.0, "<http://www.xrml.org>"
- [12] L. Pearlman, V. Welch, I. Foster, C. Kesselman, and S. Tuecke. A Community Authorization Service for Group Collaboration. Proceedings of the IEEE 3rd International Workshop on Policies for Distributed Systems and Networks, 2002.
- [13] L. Pearlman, C. Kesselman, V. Welch, I. Foster, S. Tuecke, The Community Authorization Service: Status and Future, *CHEP03, March 24-28, 2003, La Jolla, California*
- [14] Liang Fang, Dennis Gannon and Frank Siebenlist. XCAP: An Extensible Fine-grained Authorization Infrastructure for Grids, Accepted for PKI R&D 2005.
- [15] R. Alfieri, R. Cecchini, V. Ciaschini, L. dell'Agnello, A. Frohner, A. Gianoli, K. Lorente, and F. Spataro. VOMS, an Authorization System for Virtual Organizations. In European Across Grids Conference, February 2003.
- [16] D. W. Chadwick and A. Otenko. The PERMIS X.509 role based privilege management infrastructure, *Future Generation Comp. Syst. 19(2)*, pp. 27-289, 2003.
- [17] C. Ellison, B. Frantz, B. Lampson, R. Rivest, B. Thomas, T. Ylonen, "SPKI Certificate Theory", RFC 2693, September 1999, "<http://world.std.com/~cme/html/spki.html>"
- [18] PC RFC
- [19] V. Welch, I. Foster, C. Kesselman, O. Mulmo, L. Pearlman, S. Tuecke, J. Gawor, S. Meder, F. Siebenlist. X.509 Proxy Certificates for Dynamic Delegation. *3rd Annual PKI R&D Workshop, 2004*.
- [20] OASIS Web Services Security (WSS) TC, "http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss"
- [21] Shibboleth Project – Internet2, "<http://shibboleth.internet2.edu/>"
- [22] V. Welch, R. Ananthakrishnan, S. Meder, L. Pearlman, F. Siebenlist, Use of SAML in the Community Authorization Service, "<http://www.globus.org/security/CAS/Papers/SAML%20Feedback-aug19.pdf>"
- [23] Web Services Addressing Working Group, "<http://www.w3.org/2002/ws/addr/>"
- [24] OASIS Web Services Resource Framework (WSRF) TC, "http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wsrf"